COPY THE BELOW INSTRUCTION IN ITS ENTIRETY AND INSERT AS AN ATTACHMENT TO THE TASK ORDER REQUIREMENTS PACKAGE

TRICARE Management Activity
Office of Administration, Support Services Division, Personnel Security Branch
Instructions for Contractor Access to DoD IT Systems

I. BACKGROUND

The Department of Defense (DoD) requires contractor personnel designated for assignment to an ADP/IT position to undergo a successful security screening before being granted access to DoD information technology (IT) systems that contain sensitive data. Contractor personnel in positions requiring access to the following must be designated as ADP/IT-I or ADP/IT-II:

- Access to a secure DoD Facility
- Access to a DoD Information System (IS) or a DoD Common Access Card (CAC)-enabled network
- Access to DEERS or the B2B Gateway.

Effective October 1, 2009, DoD transitioned to the Electronic Questionnaires for Investigations Processing (e-QIP) for the processing of investigative Standard Forms (SFs) to include SF-85 (Questionnaire for Non-Sensitive Positions), SF-85P (Questionnaire for Public Trust Positions), and SF-86 (Questionnaire for National Security Positions). e-QIP is a web-based automated system managed by the Office of Personnel Management (OPM), which facilitates the processing of SFs for background investigations. Most companies having TRICARE contracts have positions of Public Trust and require the submission of the SF-86. The TMA, Office of Administration, Support Services Division, Personnel Security Branch (TMA PSB) coordinates with companies on the use of e-QIP. The TMA PSB shall provide each Facility Security Officer (FSO) the training necessary to access and use e-QIP.

Contractor personnel are required to initiate in e-QIP a background investigation in accordance with their position designations, which then must be favorably completed with OPM. However, the TMA PSB may approve interim access to contractor personnel for access to DoD IT systems based on a favorable advance National Agency Check (NAC) and Federal Bureau of Investigation (FBI) fingerprint check. Approval of interim access provides the contractor the opportunity to obtain a Common Access Card (CAC).

In order to safeguard against inappropriate use and disclosure of sensitive information, the following references and guidance are used by TMA as source documents:

- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- DoD 6025.18-R, "DoD Health Information Privacy Regulation, January 2003
- DoD 5200.2-R, "DoD Personnel Security Program, January 1987

- DoD 5400.11-R, "Department of Defense Privacy Program, May 14, 2007)
- DoDI 8500.1, "Information Assurance (IA)", October 24, 2002
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- Federal Information Processing Standards Publication 201 (FIPS 201-1), Personal Identify Verfication (PIV) of Federal Employees and Contractors, March 2006
- Directive Type Memorandum (DTM) 08-006, DoD Implementation of Homeland Security Presidential Directive -12 (HSPD-12), November 26, 2008
- Request for Waiver to Grant Interim Access to DoD Information Systems for TRICARE Contractor Employees, May 14, 2009
- OPM, Aligning OPM Investigative Levels with Reform Concepts, August 24, 2010
- DoD Standardized Investigation Request Procedures, November 4, 2010

The requirements above must be met by contractors and subcontractors who have access to DoD IS containing information protected by the Privacy Act of 1974 and Protected Health Information (PHI) under HIPAA.

II. PURPOSE

The purpose of this instruction is to define the Contractor's responsibilities when contractor personnel require access to DoD IT systems.

III. SCOPE OF WORK

A. **Contract/Order.** Upon notification that a contract/order has been awarded, the Contractor awarded the contract/order shall:

(1) Contact the TMA PSB and provide its company name, mailing address, e-mail address, telephone number, fax number, and the name of its designated official or Facility Security Officer (FSO).

(2) Provide its contract number, delivery order number, and contract beginning and ending dates.

B. **ADP/IT Position Sensitivity Designations.** The Prime Contractor shall ensure all contractor personnel, including any subcontractor personnel, are designated as ADP/IT-I or ADP/IT-II when their duties meet the criteria of the position sensitivity designations. The Contractor FSO shall use the guidance below to determine a contractor employee's specific ADP/IT level.

(1) **ADP/IT-I –** Those positions which have major responsibility for the planning, direction, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software; or responsibility for the preparation or approval of data for input into a system with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.

A Single Scope Background Investigation (SSBI) is the type of investigation used for ADP/IT-I Trustworthiness Determinations. The scope of the SSBI is 10 years and includes:

- Personal Subject Interview (conducted by an OPM Investigator)
- Standard National Agency Check (NAC)*
- Employment, education, residence, and reference checks
- Law enforcement and court record checks
- Check of citizenship and family's legal status (if foreign born)
- Check of spouse or cohabitants, and former spouse (if applicable)
- Credit check

(2) **ADP/IT-II –** Those positions which have theresponsibility for systems' design, operation, testing, maintenance, and/or monitoring, but are carried out under the technical review of an ADP/IT-I. Responsibilities include but are not limited to access to and / or processing of proprietary data requiring protection under the Privacy Act of 1974 or Government-developed privileged information involving the award of contracts.

A National Agency Check with Local Law and Credit (NACLC) is the type of investigation used for ADP/IT-II Trustworthiness Determinations. The scope of the NACLC is 7 years and includes the following:

- Standard NAC*
- Employment, education, residence, and reference checks
- Law enforcement check
- Credit check

**Standard NAC includes: SII, DCII, FBI name check, and FBI National Crime History fingerprint check*

Within 5-business days of notification of a contract award, the Contractor FSO shall notify and provide the Contracting Officer Representative (COR) with a list of contractor employees who require access to DoD IT systems. For each contractor employee, the list shall include the individual's name, social security number, date of birth, and the ADP/IT level.

C. **Employee Prescreening.** The Contractor shall conduct thorough reviews of information submitted on an individual's application for employment in a position that requires an ADP/IT background investigation or involves access via a contractor system to data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule. This prescreening shall include reviews that:

- Verify United States citizenship
- Verify education (degrees and certifications) required for the position in question

- Screen for negative criminal history at all levels (federal, state, and local)
- Screen for egregious financial history; for example, where adverse actions by creditors over time indicate a pattern of financial irresponsibility or where the applicant has taken on excessive debt or is involved in multiple disputes with creditors

The prescreening may be conducted as part of the pre-employment screening, but must be completed before the assignment of any personnel to a position requiring the aforementioned ADP/IT accesses. The pre-screening can be performed by the contractor's personnel security specialist, human resource manager, hiring manager or similar individual.

D. **Background Investigation Requirements.** Effective October 1, 2009, all requests for background investigations shall be submitted to OPM electronically in e-QIP. An interim DoD CAC can be given by the TMA PSB for access to DoD IT systems upon confirmation of a based on a favorable advance NAC, FBI fingerprint check, and an initiated background investigation in e-QIP.

III. ELECTRONIC QUESTIONNAIRES FOR INVESTIGATIONS PROCESSING (e-QIP)

A. **e-QIP Training and Access**.

(1) The Contractor FSO shall obtain the necessary training to access and use e-QIP.

(2) The Contractor FSO shall provide the following information to TMA PSB for e-QIP user accounts to be created:

- Social security number
- Full name
- Date of birth
- Place of birth

B. **e-QIP Role and Responsibilities.**

(1) The Contractor employee (also known as the applicant in the e-QIP process) shall:

- Be a US citizen
- Complete the security questionnaire in e-QIP within 10 calendar days from the date of invitation by the Contractor FSO
- Sign the e-QIP signature forms provided by the Contractor FSO
- Provide fingerprints electronically or by using the FD 258, Fingerprint Card
- Complete and submit the TMA CAC request form to the Contractor FSO

(2) The Contractor FSO shall:

- Be a US citizen
- Be a contractor with a minimum investigation equivalent to a NACLC
- Provide the applicant with the appropriate processing forms
- Initiate the applicant's security questionnaire in e-QIP
- Select the appropriate Agency Use Block (AUB) template in e-QIP
- Notify the COR by using e-mail that an e-QIP request has been initiated
- Inform the applicant to complete the security questionnaire in e-QIP within 10 calendar days
- Serve as the main Point of Contact (POC) for the applicant
- Monitor the e-QIP request, which includes ensuring the applicant completes the e-QIP request in designated time period
- Cancel or delete an e-QIP request on an applicant
- Request e-QIP golden question reset for applicants
- Print e-QIP signature forms and obtain signatures from the applicant
- Attach the signature forms in e-QIP before forwarding to TMA PSB for review
- Mail the applicant's original documents to include the signed e-QIP signature forms and the FD 258 to TMA PSB
- Fax the TMA CAC request form and Add User form (when applicable) to the Contractor Verification System and Common Access Card Branch (CVS/CACB)

C. **Background Investigation Request for ADP/IT-I.**

(1) A background investigation request for an ADP/IT-I position must be approved by both the COR and TMA PSB.

(2) The Contracting Company shall submit a letter on company letterhead to the COR, which includes a complete job description of the position and the justification for the ADP/IT-I designation, for approval.

(3) The Contractor FSO shall then forward the approved letter to TMA PSB for approval.

D. **Re-investigation Requirements.**

(1) Contractor personnel in ADP/IT-I and ADP/IT-II positions have re-investigation requirements. ADP/IT-I positions are re-investigated every 5 years. ADP/IT-II positions are re-investigated every 10 years. The re-investigation must be initiated within 60 days of the closed date of the prior investigation.

(2) The Contractor FSO shall track the re-investigation requirement for contractor employees. When a re-investigation is needed, the Contractor FSO shall:

- Initiate the contractor employee's security questionnaire in e-QIP
- Print contractor employee's e-QIP signature forms then obtain signatures

- Mail the e-QIP signature forms to the TMA PSB

E. **Reciprocal Acceptance of Prior Investigation.**

(1) If a new contractor personnel has a previous investigation, which meets the appropriate level of investigation required; and the break-in-service is 2 years or less, the investigation is reciprocally accepted, and no additional investigation is required.

(2) The Contracting Company shall request a verification of previous investigation from the TMA PSB, which includes the individual's name, social security number, and the closed date of the investigation. The notification may be sent to the TMA PSB by secure fax or by mail.

(3) The TMA PSB shall inform the Contractor FSO to confirm the acceptance of the previous investigation.

(4) The Contractor FSO shall notify the contractor personnel of the acceptance of the previous investigation.

F. **Notification of Employee Termination and Removal from DoD IT Systems Access.**

(1) The Contractor FSO shall notify the TMA PSB and CVS/CACB immediately when a contractor employee is terminated from a contract. The notification shall include the individual's name, the termination date, and if the individual's background investigation was initiated in e-QIP. Notification may be sent by mail, e-mail, or secure fax.

(2) The Contractor FSO shall:

- Forward a request to remove/delete the contractor employee's access to DoD IT systems
- Confiscate the DoD CAC from the contractor employee
- Return the DoD CAC to the CVS/CACB.

G. **Requests for Additional Information.**

(1) OPM may request additional information while the contractor employee's investigation is in progress. The additional information must be provided to the TMA PSB by the specified date or the background investigation may be closed. If the background investigation is closed, interim access to all DoD IT systems will be terminated.

(2) The Defense Industrial Security Clearance Office (DISCO) or the Defense Office of Hearing and Appeals (DOHA) may request additional information during the adjudication process. The additional information must be provided within the specified timeframe or the adjudication process will be stopped. If the adjudication process is stopped, interim access to all DoD IT systems will be terminated.

H. **Non-US Citizens.** Non-US citizens are not being adjudicated for TRICARE trustworthiness determinations at this time. Non-US Citizens are not allowed access to DoD IT systems unless approved by an authority designated in Appendix 6, DoD 5200.2-R. Only US

citizens shall be granted access and assigned to sensitive duties. Exceptions to these requirements shall be permitted only for compelling national security reasons (DoD 5200.2-R. C2.1.1, AP6.6.1).

I. **Notification and Mailing**. The Contractor shall use the following information to contact the TMA PSB. The Contractor shall ensure the safeguarding of any Personally Identifiable Information (PII) when transmitting any forms/documents to TMA PSB.

Mailing Address: TRICARE Management Activity
Office of Administration
Support Services Division
Personnel Security Branch
7700 Arlington Blvd., Suite 5101
Falls Church, VA 22042-5101

Secure Fax: (703) 681-6509

E-mail address: TMAPSB@tma.osd.mil